🛠️ Ejercicio: Diseño de un Informe de Hacking Ético

🎯 Objetivo del ejercicio

Simular un informe profesional de hacking ético como resultado de una auditoría controlada, aplicando los principios, metodología y estructura técnica adecuada.

🗒️ Contexto del ejercicio

Imagina que una empresa llamada **SecureBank S.A.** ha solicitado una auditoría ética de su plataforma web de banca en línea. El equipo de hacking ético ha tenido acceso autorizado para realizar pruebas controladas en un entorno de staging durante 3 días.

Tu tarea es **diseñar un informe profesional de hacking ético**, identificando al menos **3 vulnerabilidades simuladas** y aplicando recomendaciones técnicas y éticas.

📄 Instrucciones

1. Lee el escenario y asume el rol de auditor.
2. Diseña un informe completo utilizando la estructura sugerida.
3. Incluye lenguaje técnico, recomendaciones claras y respeto por el marco ético.
4. Puedes crear las vulnerabilidades ficticias o utilizar ejemplos reales de bajo riesgo.

📑 Estructura sugerida del informe

🔹 **1. Portada**

- Nombre del informe: Informe de Auditoría Ética – SecureBank S.A.
- Fecha
- Autor / equipo responsable
- Versión del documento

🔹 **2. Resumen Ejecutivo**

Breve descripción del objetivo, alcance, metodología aplicada y conclusiones principales (1 párrafo).

🔹 **3. Alcance y Limitaciones**

Define qué sistemas, aplicaciones o módulos fueron analizados, bajo qué condiciones, y qué limitaciones se establecieron (por ejemplo, sin pruebas de denegación de servicio).

🔹 **4. Metodología**

Describe la(s) metodología(s) utilizada(s), como OSSTMM, NIST SP 800-115 u OWASP, incluyendo las fases: reconocimiento, análisis, explotación y reporte.

🔹 **5. Hallazgos**

Mínimo 3 hallazgos de seguridad, estructurados así:

Vulnerabilidad	Descripción	Impacto	Riesgo (Bajo/Medio/Alto)	Evidencia	Recomendación
Inyección SQL en login	Permite acceso no autorizado	Exposición de datos	Alto	Captura de pantalla	Validación y uso de consultas preparadas
Panel de administración sin autenticación	Acceso sin login	Control total del sitio	Alto	URL directa con acceso	Restricción por roles y autenticación robusta

XSS en formulario de contacto	Inyección de scripts	Robo de sesión	Medio	Script ejecutado desde campo nombre	Sanitización de entradas

---

🔹 **6. Recomendaciones Generales**

Propuestas de mejora transversales al sistema, tales como:

- Implementar gestión de parches.
- Uso de WAF (firewall de aplicaciones web).
- Políticas de contraseñas seguras.
- Auditorías recurrentes.

🔹 **7. Consideraciones Éticas y Legales**

Asegura que todas las actividades se realizaron bajo autorización, sin afectar datos reales ni interrumpir servicios. Se mantuvo la confidencialidad y se respetó el código ético profesional (EC-Council, SANS, etc.).

🔹 **8. Conclusión**

Evaluación general del estado de seguridad de la plataforma, nivel de riesgo y prioridad de mitigación. Se destaca la necesidad de mejoras y auditorías continuas.

🔹 **9. Anexos (opcional)**

Capturas de pantalla, trazas de pruebas, herramientas utilizadas, referencias CVE.

Ejemplo:

🛡️ Informe de Auditoría Ética – SecureBank S.A.

🗓️ Fecha:

29 de marzo de 2025

👨‍💻 Equipo responsable:

CyberGuard Consultores
Analista líder: Bastián Landskron

📄 Versión:

v1.0

---

1. Resumen Ejecutivo

Se realizó una auditoría ética al sistema de banca en línea de SecureBank S.A. entre el 25 y 27 de marzo de 2025, enfocada en identificar vulnerabilidades explotables en su entorno de staging. Se aplicó la metodología OWASP Testing Guide.
Se detectaron tres vulnerabilidades críticas: inyección SQL en el módulo de autenticación, acceso sin autenticación a panel de administración y una vulnerabilidad XSS persistente. Se recomienda mitigar de inmediato los riesgos detectados.

---

2. Alcance y Limitaciones

- **Sistema auditado:** Plataforma web de banca en línea (entorno de staging).
- **Incluye:** Formularios de login, panel de administración, formularios de contacto.
- **Excluye:** Servicios de producción, APIs móviles, pruebas de denegación de servicio (DoS).
- **Permiso:** Autorización formal firmada por el CTO de SecureBank.

---

3. Metodología

Se utilizó la **metodología OWASP Testing Guide**, con enfoque en:

- Recopilación de información (Recon)
- Análisis de vulnerabilidades
- Explotación controlada
- Documentación técnica

Herramientas utilizadas: **Burp Suite**, **Nmap**, **sqlmap**, **OWASP ZAP**.

---

4. Hallazgos Técnicos

Vulnerabilidad	Descripción	Impacto	Riesgo	Evidencia	Recomendación
1. Inyección SQL en login	El campo de usuario no filtra adecuadamente las entradas. Permite acceso sin credenciales válidas.	Acceso a cuentas sin autorización	Alto	`admin' OR '1'='1` permite bypass	Usar consultas preparadas con parámetros y validación en backend.
2. Panel de administración expuesto	URL `/admin` accesible sin autenticación.	Control total del backend	Alto	Acceso directo sin login en entorno de prueba	Implementar middleware de autenticación y control de roles.
3. XSS persistente en formulario	Se permite la inyección de scripts en el campo “nombre” del formulario de contacto.	Robo de sesiones / phishing	Medio	`<script>alert('XSS')</script>` queda almacenado	Escapar y sanitizar toda entrada del usuario antes de renderizar.

---

5. Recomendaciones Generales

- Establecer un programa de **gestión continua de parches**.
- Implementar un **WAF (Web Application Firewall)**.
- Forzar uso de **HTTPS en todos los endpoints**.
- Revisar roles de acceso y segmentación de servicios internos.
- Ejecutar pruebas periódicas de penetración y revisión de código.

---

6. Consideraciones Éticas y Legales

Toda la auditoría se realizó con autorización formal, bajo un entorno controlado y sin acceso a datos reales. Se mantuvo la confidencialidad de los hallazgos. Se siguió el **Código Ético de EC-Council y SANS**, garantizando responsabilidad profesional y respeto a los marcos legales.

---

7. Conclusión

SecureBank S.A. presenta **vulnerabilidades críticas** que deben ser corregidas de inmediato. Las fallas detectadas podrían ser fácilmente explotadas en producción. Se recomienda un plan de mejora urgente y la adopción de prácticas continuas de seguridad ofensiva defensiva (DevSecOps).

---

8. Anexos

- Capturas de pantalla de pruebas
- Trazas de Burp Suite
- Scripts de prueba SQL usados en entorno de staging

📋 Instrumento de Evaluación – Ejercicio Práctico

Diseño de un Informe de Hacking Ético – SecureBank S.A.
Puntaje total: 10 puntos
Nota mínima para aprobar: 6 puntos

Criterio Evaluado	Puntaje
Informe completo con estructura sugerida (portada, resumen, metodología, hallazgos, etc.)	2 pts
Presentación de al menos 3 vulnerabilidades bien explicadas con evidencia y recomendaciones	3 pts
Claridad en la metodología aplicada (OWASP, NIST, OSSTMM, etc.)	1 pt
Propuesta de al menos 3 recomendaciones generales de seguridad técnica	1 pt
Consideraciones éticas y legales correctamente abordadas	1 pt
Conclusión técnica coherente con el análisis y riesgo evaluado	2 pts

---